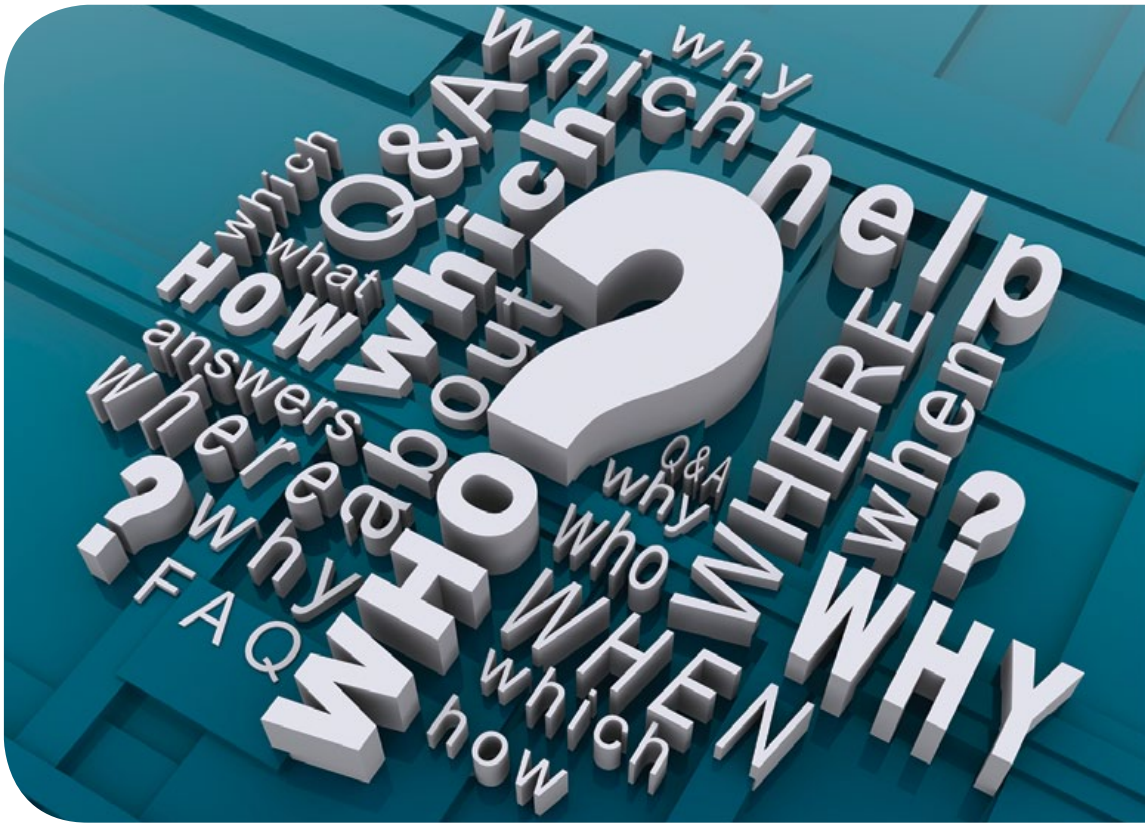

A Prolexic White Paper

12 Questions to Ask a DDoS Mitigation Provider

PROLEXIC
DDoS Attacks End Here.

Introduction

Distributed Denial of Service (DDoS) attacks continue to make global headlines, but an important facet of each incident rarely comes to light. Even though most of the targeted web sites had some level of DDoS protection in place, the attacks still succeeded:

- The web site of a leading global cosmetics retailer came under an application layer DDoS attack. The retailer fought back using the DDoS mitigation services of two of its ISPs, but the nature of the attack was too complex and its volume too large for the ISPs to handle. The site was offline and closed for business for 72 hours, resulting in more than US$1 million in lost revenue.

- When a huge DDoS attack took down the web site of a global web hosting provider, affecting 4 million customers, even the expensive DDoS mitigation hardware specifically purchased for such a scenario could not stop the attack. The e-mail customer support group and public customer forum were flooded with hundreds of thousands of complaint calls, each costing the company between US$6 and US$14 per call. To make matters worse, the hosting provider's ISP refused to bring their servers back up until a reliable DDoS mitigation solution was put in place.

- A global e-Commerce site for spa and wellness products never expected to be hit by a DDoS attack, but deployed a DDoS mitigation solution provided by its Internet hosting company to protect the site during the fourth quarter holiday shopping season. When the site was hit with a very sophisticated attack that also brought down the company's call center, the hosting company could not mitigate the attack even after four hours of downtime.

These online businesses thought they were protected against DDoS attacks, but why did their sites still go down under attack? Most likely, they underestimated the escalating strength and sophistication of today's DDoS attacks and did they not have insight into the malicious mindset of DDoS attackers and their strategy of hitting an online business at its weakest point. Most importantly, they did not understand the technical nuances of the different levels of DDoS protection and mitigation services well enough to make the most informed decision on vendor and service selection. But the most critical question is: Why did the DDoS mitigation services they had in place fail?

Knowledge is power when it comes to protecting an online business from all different types of DDoS attack. This white paper will present 12 key questions that decision makers should ask a DDoS mitigation service provider, whether a pure-play provider, ISP or Content Delivery Network (CDN), before engaging their services. It will also offer guidance to help evaluate a vendor's response to each question and what to expect in terms of DDoS mitigation services.

12 questions you must ask

Choosing a DDoS mitigation services provider is one of the most important business decisions for companies today – one that can have serious financial ramifications if not made properly. When a business web site is brought down by a DDoS attack, a company can lose millions in lost sales and lost customer confidence through the inability to provide services to online customers.

Prolexic has developed 12 key questions to ask based on our own customers' inquiries and nearly a decade of experience in successfully monitoring and mitigating all types and sizes of DDoS attacks. Most importantly, our guidance is based on our experience in what mitigation approach works and what doesn't for certain levels of attacks, as well as our keen insight into the minds and strategies of today's DDoS attackers.

1. How long have you been mitigating DDoS attacks as a service for customer environments?

This may seem obvious, but with the substantial rise in the number of DDoS attacks, more and more companies are entering the market and offering services. Most offer DDoS mitigation as an add-on service to their core business such as DNS or content delivery. While many providers will quote all kinds of statistics on network size and capabilities, one question is hard to gloss over: How long have you been mitigating DDoS attacks – not only for your own infrastructure but also for customer infrastructures? How many DDoS attacks have you successfully mitigated in customer environments? How many years have you been selling DDoS services to customers? Note that there is a big difference between experience in protecting one's own infrastructure and protecting customer environments. When it comes to mitigating attacks and outsmarting live hackers who change attack vectors and strategies in real time, experience is everything. If you don't know how to best use the resources at hand, the attacker will win – no matter how big the network is or how many staff members a mitigation provider has.

2. Where do you fit in the DDoS mitigation services market? What level(s) of protection do you offer?

The market for DDoS mitigation services is expanding dramatically as more businesses are being attacked and as the volume and complexity of attacks escalate. To respond to the continuing surge in DDoS activity, two broad types of DDoS mitigation providers have emerged:

- Pure play providers whose core business is DDoS mitigation and who offer both an emergency proxy service and a routed service, as well as other specialized monitoring and analysis services
- Add-on providers such as Content Delivery Networks (CDNs), Internet Service Providers (ISPs), hosting companies, and telecom companies who provide DDoS mitigation solutions either bundled with core services or as an add-on, usually only as a proxy service

A CDN's core business is content acceleration, not DDoS protection. As a result and unlike pure play providers, CDNs typically do not offer full back end protection and do not support all protocols. The same can be said for ISPs and telcos, which have different strengths, but also significant weaknesses that undermine their ability to offer 100 percent protection against all types of DDoS attacks.

3. How do you protect against attacks that are directed at routers, firewalls, IPs, and application services directly?

Attackers are smart and have many ways of bypassing DDoS defenses. One powerful technique that attackers employ is spoofing trusted IP addresses. Spoofing refers to the creation of IP packets with a forged source IP address - often from a known, trusted source such as partners and vendors. Even your own IP address can be spoofed. These spoofed attacks are designed to bypass simple white lists and can be used to launch a volumetric attack that will fill up all of your Internet connections and bring your site down. Because these attacks come in at the back door, they bypass any cloud services you might engage, such as CDNs.

Attackers also use sophisticated methods to overflow a site with legitimate looking requests coming from a large botnet. These requests pass through firewalls and Access Control Lists (ACLs) because they look like legitimate traffic. The only way to identify and block the malicious traffic is through comprehensive traffic analysis to identify group behavior. Ask your provider how they block large volumes of legitimate looking requests, especially if those requests are coming in at a fairly low rate.

In addition to the two types of attacks described above, attackers are constantly developing and distributing new DDoS platforms and tools specifically designed to bypass current DDoS defenses. Therefore, ask your DDoS mitigation provider if they have a research team in place that focuses on identifying and proactively developing new, next generation DDoS mitigation solutions to counteract the latest DDoS tools and techniques before they become widespread. Unfortunately, companies that offer DDoS mitigation as an add-on service will not have these resources in-house.

Protecting against these types of subtle attacks is not easy. It requires a routed-based solution that works at the network layer rather than at the proxy layer alone. Only a mitigation system that can intercept all of the traffic, both legitimate and spoofed, and analyze it with a state-of-the-art system and the expertise of live DDoS analysts can stop them.

4. Do you monitor our routers for volumetric attacks in the above cases?

It is difficult for CDNs, ISPs, and hosting providers – or any other entity that offers DDoS mitigation as an add-on service – to perform dedicated DDoS monitoring for each customer. For example, the largest CDNs have literally hundreds of thousands of servers located in thousands of locations around the world to do what they do best – accelerate the delivery of web content close to the source of user requests. As CDNs do not usually have a dedicated DDoS monitoring and mitigation team of experts on hand, monitoring routers for volumetric attacks is likely to be inconsistent, while response time and time-to-resolution is likely to be slower than a pure play provider, even though the CDN may offer a proxy DDoS mitigation service.

A routed DDoS mitigation solution with flow based monitoring ensures protection against Layer 3 and Layer 4 volumetric attacks on edge routers and other threats to back door applications. Usually provided as a subscription service, flow based monitoring enables early detection and notification of TCP abuse, UDP floods, and ICMP floods by directly monitoring edge routers. This service should include continuous expert live monitoring by experienced DDoS mitigation technicians rather than by an automated mitigation appliance. In addition, the flow based monitoring service should be backed by a robust time-to-notify SLA, as well as provide secure access to network analysis tools through a customer portal to ensure you can take proactive defensive measures within minutes of an attack beginning.

5. What protection do you offer protocols other than HTTP, HTTPS, and DNS? What about VPN endpoints?

Be aware that all protocols are not protected by a proxy DDoS mitigation service, especially if you have VPNs employing a varied range of protocols in a large number of locations. Proxy mitigation solutions offered by ISPs, CDNs, and others as add-on services protect only HTTP, HTTPS, and DNS protocols. Again, only a pure play DDoS mitigation services provider can offer an enterprise-routed platform with the dedicated bandwidth, sophisticated analysis tools, and live team of experts to protect VPN endpoints and any type of protocol.

6. Do you have an SLA guaranteeing mitigation within a certain time period?

Minutes count during a DDoS attack. For example, industry analyst firms estimate the cost of a 24-hour outage for a large e-Commerce company can approach US$30 million. Not many businesses can afford to take that risk, which is driving the need for DDoS mitigation services. However, as the failure scenarios described earlier prove, proxy DDoS mitigation from an ISP or hosting service is inadequate especially when fighting randomized Layer 7 attacks in which live attackers constantly change signatures and protocols. Denial of service attacks that should be mitigated quickly – that is, to bring a web site back up and/or restore certain services – can take an ISP or CDN days or weeks, and they sometimes fail completely.

Therefore, a robust time-to-mitigate SLA should guarantee mitigation to restore web site services in a specified timeframe, often 30 minutes or less once traffic starts flowing through the mitigation network. In addition, the SLA should protect against DDoS attacks on all customer servers, all IP addresses, all upstream carriers, all global web sites, and all protocols. Only a pure play provider that offers DDoS mitigation as its core service can fulfill this vast range of protection under a single SLA.

7. Can you perform real-time analysis of our web traffic and precisely describe what the attack is? Especially if it is a custom targeted attack by a smart adversary?

Today's DDoS attackers are especially smart and cunning – and unfortunately many companies underestimate the damage they can do. First of all, smart attackers may start out testing the strength of your DDoS defenses with a volumetric attack, then switch midstream to more sophisticated

measures that bypass all automated mitigation tools and target the application layer – the most devastating type of attack. Whether bandwidth floods or slower volume attacks that appear to be legitimate traffic, the sooner a DDoS mitigation provider can analyze the traffic and identify the attack type, the more quickly mitigation can begin.

Real-time analysis and response by live DDoS mitigation technicians is paramount to outsmarting live attackers who are focused on targeting a company's weakest point. Real-time means that technicians can analyze the traffic in great detail with very rapid turnaround to reinforce an SLA. In addition, an experienced live mitigation team can respond in real-time to signature changes during an attack campaign, thus mitigating the attack much faster than using automated tools alone. ISPs, CDNs, hosting services, and other add-on service providers do not have the expertise and DDoS specific technology to achieve the needed level of granularity.

So be sure to ask if the DDoS services provider is able to look at all of the traffic and at what level are they able to analyze it. Beyond that, you should make sure that the provider can also identify the attack type and mitigate it. Also, be wary of providers who say they have automated rules for mitigation, because DDoS mitigation is not a one-size-fits-all exercise. It is best to have a provider who can tailor rules specifically on an attack-by-attack basis, especially if a motivated attacker rapidly changes attack signatures. That is the only way you can be sure to minimize false positives and ensure that rapidly changing attack signatures can be dealt with quickly.

8. How long does it take to push out a filtering rule?

An experienced mitigation provider will be able to quickly analyze a complex, randomized Layer 7 attack, develop and test a custom signature tailored to defeat the attacker's specific countermove, and deploy it globally. Even though automated mitigation systems can respond faster in non-randomized attacks, they create a large number of false positives and have a tendency to break some aspect of the application they are supposed to defend. Responding to a live attacker with human-driven, precisely engineered countermeasures is where a pure play mitigation service provider has the edge over an ISP or hosting provider.

Even if a mitigation services provider has the latest automated tools, the best workflow for pushing out filtering rules is custom signature deployment guided by live DDoS mitigation experts. A typical CDN, for example, using only automated tools would need at least an hour to create and deploy new filtering rules – and an hour is a very long and costly time when you consider that a popular e-Commerce company and Prolexic client estimated one second of web site downtime from a DDoS attack would cost US$1,000.

9. Do you have automatic DDoS responses like active challenges? If so how can you guarantee they do not break applications?

Automated DDoS mitigation responses or active challenges should be the last resort in a DDoS defense strategy. Simply put, mitigation appliance algorithms do not know your applications or your customer experience. Too often they over-mitigate, creating false positives or incorrect identification

of attackers. The impact of overmitigation can result in blocking legitimate customers, affecting advertising systems, and lowering SEO rankings to the extent that they can block all traffic to the site.

Rather than relying on an automated algorithm, the best and safest DDoS defense is to have traffic analysis and mitigation implemented by human experts and skilled technicians who monitor your traffic accurately, on a case-by-case basis and take nothing for granted. This provides the lowest chance of false positives, saving you from devoting valuable resources to debugging applications during a DDoS attack and blocking legitimate traffic. A live mitigation team can fingerprint the attack aimed at your web site and answer the attacker in real-time with a targeted signature. Automated solutions use simplistic formulas for auto-blocking that cause problems in the real world. Simply put, no DDoS defense solution should cause application problems when invoked.

10. Can your staff inspect our SSL traffic manually? What does this mean for privacy?

Consider it a red flag if a DDoS mitigation vendor answers affirmatively to the first part of this question without giving you any supporting details on how the inspection is performed. Typically, ISPs or CDNs require you to share SSL keys and they will deploy them on thousands of geographically dispersed servers. This increases the risk of encryption keys being compromised and subsequent exposure to masquerading if data centers are compromised by a data exfiltration attack.

You should never be asked to compromise the integrity of your SSL keys and infrastructure to a DDoS mitigation vendor. Instead, a vendor should be able to offer credible audited proof that its SSL key management practices provide the highest levels of assurance and operate within international privacy laws. Ask if they have achieved PCI compliance or comparable certification status.

11. How long does it take for DDoS attack detection and notification?

Most CDNs and ISPs are simply too large and do not have the dedicated DDoS mitigation resources to detect a DDoS attack against a single site, let alone notify the customer. Often, their mitigation services are basic with poorly detailed alerts and a fairly generic analysis component. Most importantly ISP and CDN networks are not designed specifically for analyzing and fighting complex cyber attacks. Even if they offer protection against volumetric attacks, they have no resources for identifying and analyzing targeted Layer 7 attacks.

The response time of a pure play DDoS mitigation provider is far superior to what other organizations can provide. The monitoring workflow is designed to quickly detect DDoS traffic anomalies, analyze them, and offer an SLA guaranteed response time to notify customers of possible DDoS attacks. Again, this service requires live monitoring by a team of DDoS mitigation experts as part of a mitigation solution. Detection of volumetric attacks against Internet circuits and routers requires flow-based monitoring services. Detection of Layer 7 application-based attacks requires a different monitoring and analysis approach. Ask your mitigation provider how long it takes to receive notification for different attack types and ask if there are attack types they cannot detect. Also question how detailed the alerts are – are they generic and automatic without ever passing through an interpretive layer of analysis or are the alerts qualified by DDoS mitigation experts?

12. Do you provide detailed attack reports during and after an attack? If after, how long does it take to prepare a report?

Staying informed and working closely with a DDoS mitigation services provider is a good way to take a proactive stance against DDoS attacks. Once the mitigation service is activated, the provider should record detailed attack reports, including all of the real IP addresses blocked in the attack, stored in a database that is instantly accessible to you through a secure online customer portal. Generally, proxy mitigation services offered by CDNs and ISPs do not include any detailed reporting either during or after an attack.

Conclusion: Knowledge leads to success

Like a playground bully, DDoS attackers are very aggressive and smart and will detect and attack weaknesses. Companies with proxy DDoS protection through their ISP, CDN, or hosting company may believe that they have a strong defense against these bullies, but time after time the attackers win when they attack edge routers, applications – including the use of SSL – and upstream ISPs – the most difficult areas to protect. The DDoS mitigation failures in the introduction of this paper are prime examples, but they can be turned into success stories with a routed DDoS mitigation solution from an experienced pure play vendor like Prolexic.

With that said, an informed approach is to take advantage of what ISPs and CDNs do best – enabling reliable connectivity with end users and accelerating the delivery of web content – and marry that expertise with routed DDoS mitigation services from a pure play vendor with a high-level of experience, success and precision in DDoS mitigation.

Prolexic believes that the best defense against DDoS is a proactive strategy that includes educating oneself on the types of attacks, the mindset of the attackers, and the pros and cons of each type of attack mitigation service. Then ask a DDoS mitigation services provider these 12 tough questions and apply critical thinking to select the best solution that truly protects your entire network 100 percent of the time.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit **www.prolexic.com**, follow **@Prolexic** on Twitter, email **sales@prolexic.com**, or call **+1 (954) 620 6002**.

v.071212

PROLEXIC
DDoS Attacks End Here.